CLAIMS

What is claimed is:

1. A method performed by a user terminal of a wireless access network, the method comprising:

scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network; and

sending a message to the access point, the message including the scrambled user terminal certificate.

2. The method of claim 1, further comprising generating the shared secret and providing the shared secret to the access point.

3. The method of claim 1, wherein providing the shared secret to the access point comprises the message further including the shared secret encrypted with an access point public key.

4. The method of claim 1, wherein scrambling the user terminal certificate using the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

5. The method of claim 4, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

6. The method of claim 5, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

7. A user terminal comprising:

a memory to store a user terminal certificate;

a processor coupled to the memory to scramble the user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network; and

a transmitter coupled to the processor to send a message to the access point, the message including the scrambled user terminal certificate.

8. The user terminal of claim 7, wherein the processor is also to generate the shared secret and the transmitter is also to provide the shared secret to the access point.

9. The user terminal of claim 7, wherein the transmitter provides the shared secret to the access point by including in the message the shared secret encrypted with an access point public key.

10. The user terminal of claim 7, wherein the processor scrambles the user terminal certificate using the shared secret by combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

11. The user terminal of claim 10, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

12. The user terminal of claim 11, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

13. A method performed by an access point of a wireless access network, the method comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, and a user terminal certificate scrambled using the shared secret;

decrypting the shared secret using an access point private key; and

unscrambling the user terminal certificate using the decrypted shared secret.

14. The method of claim 13, wherein unscrambling the user terminal certificate using the shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

15. The method of claim 14, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

16. The method of claim 15, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

17. The method of claim 13, wherein the user terminal certificate includes an identification of the user terminal and a user terminal public key which corresponds to a user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal.

18. An access point comprising:

a receiver to receive a message from a user terminal, the message containing a shared secret encrypted with an access point public key and a user terminal certificate scrambled using the shared secret; and

a processor coupled to the receiver to decrypt the shared secret using an access point private key, and unscramble the user terminal certificate using the decrypted shared secret.

19. The access point of claim 18, wherein the processor unscrambles the user terminal certificate using the shared secret by combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

20. The access point of claim 19, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

21. The access point of claim 20, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

22. The access point of claim 18, wherein the user terminal certificate includes an identification of the user terminal and a user terminal public key which corresponds to a user terminal private key, wherein the access point authenticates the user terminal by checking the user terminal certificate.

23. A machine-readable medium storing data representing instructions that, when performed by a processor of a user terminal, causes the processor to perform operations comprising:

scrambling a user terminal certificate using a shared secret to be known only by the user terminal and an access point of the wireless access network; and

sending a message to the access point, the message including the scrambled user terminal certificate.

24. The machine-readable medium of claim 23, wherein the instructions further cause the processor to perform operations comprising generating the shared secret and providing the shared secret to the access point.

25. The machine-readable medium of claim 23, wherein providing the shared secret to the access point comprises the message further including the shared secret encrypted with an access point public key.

26. The machine-readable medium of claim 23, wherein scrambling the user terminal certificate using the shared secret comprises combining the user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret.

27. The machine-readable medium of claim 26, wherein the part of the shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

28. The machine-readable medium of claim 27, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

29. A machine-readable medium storing data representing instructions that, when performed by a processor of an access point, causes the processor to perform operations comprising:

receiving a message from a user terminal of the wireless access network, the message containing a shared secret encrypted with an access point public key, and a user terminal certificate scrambled using the shared secret;

decrypting the shared secret using an access point private key; and

unscrambling the user terminal certificate using the decrypted shared secret.

30. The machine-readable medium of claim 29, wherein unscrambling the user terminal certificate using the shared secret comprises combining the scrambled user terminal certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the decrypted shared secret.

31. The machine-readable medium of claim 30, wherein the part of the decrypted shared secret used to initialize the linear feedback shift register is not used for symmetric key cryptography between the user terminal and the access point.

32. The machine-readable medium of claim 31, wherein the remainder of the shared secret is used for symmetric key cryptography between the user terminal and the access point.

33. The machine-readable medium of claim 29, wherein the user terminal certificate includes an identification of the user terminal and a user terminal public key which corresponds to a user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal.